International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-8, Issue-6, June 2018

Security Enhancement of Misbehavior Nodes in Vehicular Ad-Hoc Networks Using Hash Function

Priyanka Tiwari, Mr. Rahul Gupta

Abstract— **Communication within Vehicular ad hoc Network relies over exchange over data among unique vehicular nodes among the network. This helps to enhance the safety, riding efficiency yet comfort regarding the trip of the travellers. In that network, information acquired beside cars is utilized in conformity with improved majority of the decisions. VANETs bear in modern times been set up namely reliable networks up to expectation because of cars utilization through verbal exchange motive over highways then civic environments. Along with the benefits, like occur a tremendous range of challenges in VANET such that provisioning concerned QoS, high connectivity, bandwidth, protection to vehicle and single privacy. This article provides cutting-edge regarding VANET and discusses the related issues.**

An imperative need regarding the nodes is in accordance with assist along each vehicle for successful data transmission. Thus, the impact regarding malicious yet selfish users need to keep detected after ensure the operations over Vehicular Ad Hoc Network. In this article, we proposed On-demand Misbehavior Detection approach in vehicular communication. We adapt two location-based routing protocols, greedy perimeter stateless routing and adhoc on demand distance vector routing protocols, in conformity with our On-demand Misbehavior Detection. Various experiments are performed to show the usefulness and efficiency concerning the proposed On-demand Misbehavior Detection technique. The simulation and analytical results confirmed that proposed technique is very effective for detecting malicious nodes.

Index Terms—**Vehicular Ad Hoc Networks (VANET), misbehavior detection, VANET Routing, Modeling**

I. INTRODUCTION

Intelligent Transport Systems (ITS) perform use of communication, network and information technology to enhance the mobility, quality, comfort and safety for smart cities [1]. For the development over ITS, Vehicular Ad-Hoc Network (VANET) is regarded namely a backbone because of all its functions and attracted researchers from each industry and academia all over the worls [2], [3]. VANET has the potential to improve vehicle safety on the roads efficiency of traffic and comfort to commuters [4]. In VANETs, the information exchange occurs among vehicles no longer solely between an ad-hoc primarily based Vehicle-to-Vehicle (V2V) communication however also in a Vehicle-to- Infrastructure (V2I) then Infrastructure-to-Infrastructure (I2I) communication as shown in figure 1. Various roads with moving vehicles are are shown in the figure along with roadside infrastructure used for I2I or V2I communication.
Although Vehicular Ad-hoc Network (VANET) is no longer an instant topic, it continues to provide current lookup challenges and problems. The predominant goal of VANET is to help a group of vehicles to communicate and establish a network without the help of central administrator or controller. One of the foremost features of VANET is used in critical medical emergency situation where there is no infrastructure to pass the information for saving the human lives. However, along with it useful purposes concerning VANET, instant challenges or problems may arise. Lack of infrastructure of VANET puts additional duties on vehicles. Every vehicle becomes part of the network yet additionally manages or controls the communication of this community along including its own communication requirements. Vehicular ad-hoc networks are responsible for the conversation among moving vehicles for a stable environment. A vehicle can communicate with another vehicle directly which is called Vehicle to Vehicle (V2V) communication, or a vehicle can communicate to an infrastructure such as a Road Side Unit (RSU), known as Vehicle-to-Infrastructure (V2I). Figure 1 shows a typical VANETscenario.

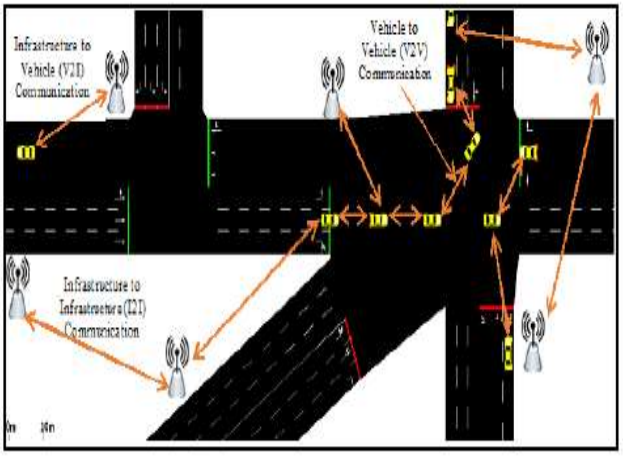

Figure 1 Various Types of Communication in VANETs

Many more advanced routing strategies have been developed for vehicular networks in recent years. To aid the process of establishing and controlling communication connections, location information (i.e. via Global Positioning System (GPS)) is used in some of the routing techniques. For example, into the fully location based approach, each forwarder selects the subsequent forwarding node by the use comparing the positions concerning all its neighbors for a destination by a source or an intermediate node. This position information is obtained through periodic broadcasts from neighboring nodes. Some of the location-based approaches are Connectionless Approach (CLA), Contention-Based Forwarding (CBF), Greedy Perimeter Stateless Routing (GPSR), and Trajectory-Based Forwarding (TBF).
Although establishing and maintaining communication links are important tasks in VANET, many works 5–8 have pointed

Priyanka Tiwari , Department of Computer Science and Engineering, M.Tech Scholar, Kanpur Institute of Technology, Kanpur, India.
Mr. Rahul Gupta, Assistant Professor, Department of Computer Science and Engineering, Kanpur Institute of Technology, Kanpur, India

out that the impact of malicious and selfish users must also be carefully considered. In most of VANET routing protocols, all vehicles (often called nodes) are required to participate in the routing and data forwarding process. However, it may be subjected to malicious attacks because of lack of infrastructure and centralized administration. Malicious users can drop, modify, or misroute data packets. The purpose of the malicious node is to attack network using various penetration techniques. As the result, the availability and robustness of the network are highly compromised. The proposed routing protocol is introduced in section ''PRAPOSED ROUTING PROTOCOL.'' In section ''Experimental results,'' we present our experiments with simulation and analytical results. Finally, we conclude this article and discuss future works in section ''Conclusion and future work.''

II. EVOLUTION OF VANETs

In Vehicular ad-hoc networks, the term "Ad-hoc" is a Latin word with the meaning "for this purpose" [5]. Here, the network consists more than one nodes that are linked through wireless links. In ad-hoc networks the links may connect or detach frequently. So, for managing the property of robustness, reliability, efficiency, timeliness and scalability ventures within ad-hoc network, dynamic restructuring required to be handled by means of the underlying network [6]. For this, the network should send the information with the help of other nodes of the system to establish the communication among various pair of nodes. A wireless ad-hoc network is an ad-hoc network in which all communication links are wireless. The main features of a Wireless Ad-hoc NETwork (WANET) are absence of pre-existing infrastructure and fixed base stations; transmission within link coverage and mobile nodes with dynamic connections.

Classification of wireless ad-hoc networks

Wireless ad-hoc networks [14] being porposeful and economical can be used in emergency situations like military conflicts or natural disasters due to their very less configuration requirement and quick deployment at large scale. Wireless ad-hoc networks are further evolved into three subcategories, according to their use in various applications as shown in Figure 2.

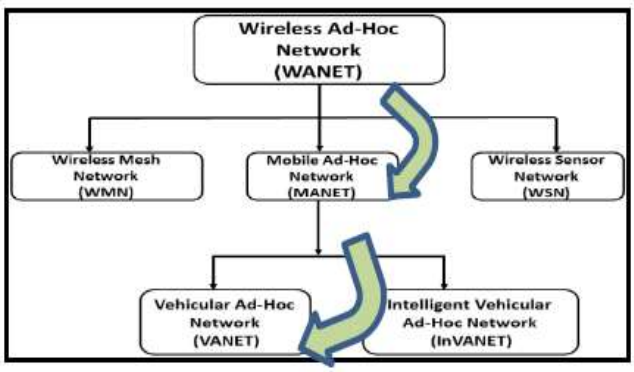

Figure 2: Evolution of VANETs

The three categories of Wireless ad-hoc networks (WANETs) are:

- Wireless Sensor NETworks (WSNs)
- Wireless Mesh NETworks (WMNs)
- Mobile Ad-hoc NETworks (MANETs)

Figure 2 depicts that VANET is a subclass of MANET that further a subclass of WANETs. VANET are formed with vehicles as nodes in contrast to MANET that uses mobile phones/laptops. A Mobile Ad-hoc NETwork (MANET) is an infrastructure-less and self-configuring network of mobile nodes coupled through wireless links. Every node in a MANET can move independently in any direction, and hence links of that node with other nodes in the network may change very frequently.

A. *Overview of VANET*

In Vehicular Ad-Hoc NETwork (VANET) moving vehicles are considered as nodes and the distance between them on the roads is considered as edges in the network.

Each vehicle can accept and transfer the messages from other vehicles or road infrastructure with the help wireless medium [7]. All participating vehicles can be considered as a wireless nodes or routers, allowing them to connect and communicate in the range of approximately 100 to 500 meters and forms a network [1], [8]. When a vehicle falls out of the signal range, it will be dropped out of the network. Any other vehicles can join the network, when it comes in the signal range of the existing vehicles in the network [9]. These vehicles are enbuild with advanced wireless communication devices known as On Board Units (OBUs) and have no base stations assigned to them [10].

These OBUs are responsible for V2V yet V2I communications. Intelligent Transportation System (ITS) is the most important application supported through vehicular ad-hoc networks. Another vital application of VANETs is in imitation of behave along safety. For example, suppose a road accident is detected by any vehicle then this information about the accident must be forwarded to other neighboring vehicles present in the system. The use over security messages is that they should stay delivered in conformity with every neighboring node without much delay i.e. inside restricted time. If an individual event-driven message is misplaced or security message is delayed, this may lead to loss of life [11]. ITS uses the WAVE protocol for decreasing inconveniences and avoiding danger situations like prevention and/or detection of various accidents [12]. ITS may can also be used for distributing data or information touching the street maintenance, climate forecasts then road conditions alongside including emergency notifications.

III. MISBEHAVIOR NODES DETECTION IN VANETs

Information dissemination in VANETs happens through cooperative behaviour of the vehicular nodes. Messages transmitted in vehicular network carry vital information like traffic jam, emergency brake events, road conditions, accident notifications, bad weather conditions, etc. In such a case, if any vehicle act maliciously and tamper with the messages, the results may be very dangerous. Thus misbehaviors in VANET is a very crucial issue. Misbehavior can be generally referred to as any kind of abnormal behaviour that is deviation from the average behaviour of other vehicular nodes in the VANETs. Hence, detection of misbehaviors and the malicious vehicular nodes involved in such misconducts is extremely imperative, in order to make VANET a secure network. A lot of work has been carried out to detect misbehavior and malicious nodes in Vehicular ad hoc networks. The misbehavior detection schemes can be broadly

classified into following types: Node-centric and Data-centric misbehavior detection schemes as shown in Fig. 3. differentiates them. Some of the contributions of the researchers under the classification schemes mentioned above are discussed in this section. Considering the numerous advantages of VANETs and hazardous consequences that could result due to misbehavior, security of VANETs has become a prominent area of research.

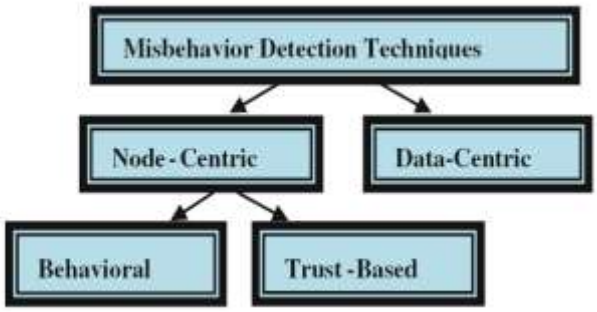

Figure 3: Taxonomy of misbehavior detection techniques in VANETs

IV. ROUTING PROTOCOLS

In VANET, the routing protocols are classified into five categories: Topology based routing protocol, Position based routing protocol, Cluster based routing protocol, Geo cast routing protocol and Broadcast routing protocol. These protocols are characterized on the basis of area / application where they are most suitable [13].

A. Topology Based Routing Protocols

These routing protocols use links information that exists in the network to perform packet forwarding. They are further divided into Proactive and Reactive.

(i) Proactive routing protocols

The proactive routing means that the routing information, like next forwarding hop is maintained in the background irrespective of communication requests. The advantage of proactive routing protocol is that there is no route discovery since the destination route is stored in the background, but the disadvantage of this protocol is that it provides low latency for real time application. A table is constructed and maintained within a node. So that, each entry in the table indicates the next hop node towards a certain destination. It also leads to the maintenance of unused data paths, which causes the reduction in the available bandwidth. The various types of proactive routing protocols are: LSR, FSR.

i) Reactive/Ad hoc based routing

Reactive routing opens the route only when it is necessary for a node to communicate with each other. It maintains only the routes that are currently in use; as a result it reduces the burden in the network. Reactive routing consists of route discovery phase in which the query packets are flooded into the network for the path search and this phase completes when route is found. T he various types of reactive routing protocols are AODV, PGB, DSR and TORA.

B. Position Based Routing Protocols

Position based routing consists of class of routing algorithm. They share the property of using geographic positioning information in order to select the next forwarding hops. The packet is send without any map knowledge to the one hop neighbor, which is closest to destination. Position based routing is beneficial since no global route from source node to destination node need to be created and maintained. Position based routing is broadly divided in two types: Position based greedy V2V protocols, Delay Tolerant Protocols.

i) Position Based Greedy V2V Protocols

In greedy strategy an intermediate node in the route forward message to the farthest neighbor in the direction of the next destination. Greedy approach requires that intermediate node should possessed position of itself, position of its neighbor and destination position. The goal of these protocols is to transmit data packets to destination as soon as possible that is why these are also known as min delay routing protocols. Various types of position based greedy V2V protocols are GPCR, CAR and DIR.

ii) Greedy Perimeter Coordinator Routing (GPCR)

GPCR is based upon the fact that city street form a natural planner graph. GPCR does not require external static street map for its operation. GPCR consists of two components: A Restricted Greedy forwarding procedure, and a repair strategy for routing algorithm. A GPCR follows a destination based greedy forwarding strategy, it routes messages to nodes at intersection. Since GPCR does not use any external static street map so nodes at intersection are difficult to find. GPCR uses heuristic method for finding nodes located at intersections and designates those nodes as coordinators. Coordinator has the responsibility of making routing decisions. There are two approaches used for coordinator determination they are:

(a) Neighbor Table Approach: The nodes periodically transmit beacon messages which contains their position information and last known position information of all neighbors, by listening to beacon messages a node as information about its own position, position of its neighbor and neighbor's neighbor. Using this information node X consider itself to be within the intersection.

(b) Correlation coefficient approach: In this case node uses its position information and the position information of its immediate neighbor to find the correlation coefficient, p_{xy}. This approach performs better than neighbor table approach. By using this approach the algorithm can avoid dependencies on external street map.

C. Cluster Based Routing

Cluster based routing is preferred in clusters. A group of nodes identifies themselves to be a part of cluster and a node is designated as cluster head will broadcast the packet to cluster. Good scalability can be provided for large networks but network delays and overhead are incurred when forming clusters in highly mobile VANET. In cluster based routing virtual network infrastructure must be created through the clustering of nodes in order to provide scalability. The various Clusters based routing protocols are COIN and LORA_CBF.

D. Broadcast Routing

Broadcast routing is frequently used in VANET for sharing, traffic, weather and emergency, road conditions among vehicles and delivering advertisements and announcements. The various Broadcast routing protocols are BROADCOMM, UMB, VTRADE, and DV-CAST.

E. Geo Cast Routing

Geo cast routing is basically allocation based multicast routing. Its objective is to deliver the packet from source node to all other nodes within a specified geographical region (Zone of Relevance ZOR). In Geo cast routing vehicles outside the ZOR are not alerted to avoid unnecessary hasty reaction. Geo cast is considered as a multicast service within a specific geographic region. It normally defines a forwarding zone where it directs the flooding of packets in order to reduce message overhead and network congestion caused by simply flooding packets everywhere. In the destination zone, unicast routing can be used to forward the packet. One pitfall of Geo cast is network partitioning and also unfavorable neighbors, which may hinder the proper forwarding of messages. The various Geo cast routing protocols are IVG, DG-CASTOR and DRG.

V. PROPOSED ROUTING PROTOCOL

Greedy Forwarding Algorithm Implementation

Greedy forwarding strategies can run into a situation called local maximum or local optimum, in which the sending vehicle is closer to the destination than all of its neighbours, and the destination is not reachable by one hop. However, this does not mean that there is no connectivity to the destination (Figure 4) and so, when a local maximum occurs, a recovery strategy is used. The recovery-mode strategy used by GPSR is the right-hand rule, commonly used to traverse graphs. In [49] the authors refer to this recovery-mode strategy as Perimeter mode. As per this rule, if node n receives a packet from edge E1, it sends the packet through its next edge counter-clockwise about n. The routing protocol switches back to forwarding mode once the forwarding node is closer to the destination than the node that triggers the recovery-mode strategy.

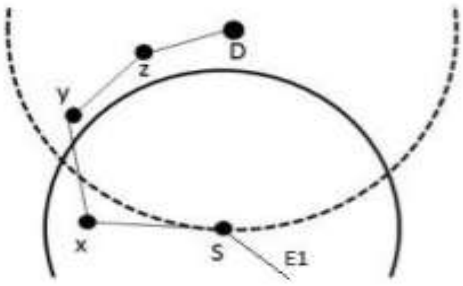

Figure 4 Local-maximum situation

Each vehicle periodically updates its neighbor's details or neighbors tables. Source vehicle finds the shortest path to the destination vehicle by enabling route discovery process. Greedy Forwarding algorithm is implemented to transfer the message by finding the node that is closest to the destination.

The GPSR algorithm is described using pseudo-code in Algorithm, wherein:

- R, is the node receiving a packet p for Destination D.
- N, is the set of one-hop neighbours of R.
- n, is a node of the set N that is used to forward the packet.
- D, is the destination of the packet

4.3.2 Pseudo code for GPSR Routing Protocol

if n ∈N: Distance (n, D) ≤Distance (R, D) then
{Greedy forwarding}
n = Min_Distance(N, D)
Forward_packet (p, n)
Return
else
{local-maximum, use right-hand rule}
n = Right_Hand_Rule(N)
Forward_packet (p, n)
Return
End if

Above pseudo code describes that source finds the shortest path to reach the destination by following Greedy Forwarding algorithm. Else if the sender vehicle itself is close than all its neighbors and destination not reachable by one hop i.e., attains local-maximum situation then right hand rule is followed to forward packets. As per this rule, if node n receives a packet from edge E, it sends packet through its next edge counter-clockwise about Proposed Gpsr Algorithm propsed Gpsr is a position-based routing protocol which consists of two modes, yet using an advance greedy forwarding. As obstacles (e.g. buildings) block radio signals, packets may only be greedily forwarded along road segments as close to the destination as possible and finding the direction. Accordingly, the major directional decisions are made using the neighbors broadcast table. When packets reach a local maximum, a point at which there is no node closer to the destination, the node switches to proposed Gpsr recovery mode (i.e. Perimeter Mode).Bellow shows the algorithm of proposed Gpsr.

4.3.3 Proposed GPSR Algorithm

At source:
mode = greedy
Intermediate node:
if (mode == avdgreedy)
{
Advance greedy forwarding;
if (fail) mode = avdperimeter;
}
if (mode == avdperimeter) {
if (have left local maxima) mode = greedy;
}

VI. RESULTS

The performance of routing protocols is measured through performance metrics including the throughput, end-to-end delay and the packet delivery ratio. In general, as the traffic load increases, the routing protocol needs to transport more data across the network, which causes more transmissions on the wireless medium, resulting in more collisions and packet losses. Similarly, high mobility also strains performance of the rp (routing protocols) by involving constantly changing

routes. The end-to-end delay is also higher of high traffic, mobile topologies since there are a large number of collisions, which requires more frequent retransmissions at the link layer, resulting in long delays. In particular, the end-to-end delay is also tightly coupled with the network size since a large network has longer routes on average, requiring more hops and consequently, more delay.

Packet Delivery Ratio: The PDR percentage represents the percentage of total sent packets from source node, which are transmit successfully data received at the destination nodes.

Packet Loss Ratio: The Packet Loss Percentage (or Ratio) represents the total number of packets lost in the network between source and destination nodes.

Aggregate Throughput: The aggregate throughput is calculated the Total no. of bytes successfully received at the sink divided by the total time duration. This aggregates all the flows in the network.

Average End to End Delay: The average delay is the averaged results of how much time consume it takes a packet to go from the start point to the destination.

Routing Over-head: In this measure of routing packets (non-data) generated by the protocol.

Figure 5 represents the average end to end delay where, x-axis represents the no. of nodes and y-axis delay time. In this graph shows how much time consume it takes a packet to go from the start point to the destination by using malicious_AODV and secure_AODV and proposed GPSR methods. The end-to-end delay which is the average time it takes for a packet to traverse the network from its source to destination. Our routing solution shows a low end-to-end delay because the packet is recovered by the carry-end-forward recovery mode where the data packet is carried until the carrier node finds a neighbor closest to the destination or it reaches itself the destination. In case of the local optimal, AODV tries to find a new route which is very difficult to keep it in a high dynamic environment and this increase its delay time. GPSR uses the right-hand rule to recover packet from local optimal.

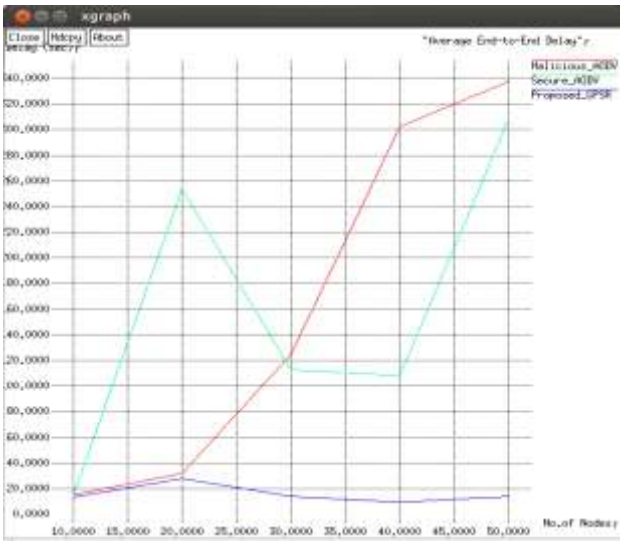

Figure 5: VANET Delay

Figure 6 represents the energy consumption where, x-axis represents the no. of nodes and y-axis represents the energy consumption. In this graph shows how much energy consume it takes a packet to go from the start point to the destination by using malicious_AODV and secure_AODV and proposed GPSR methods.

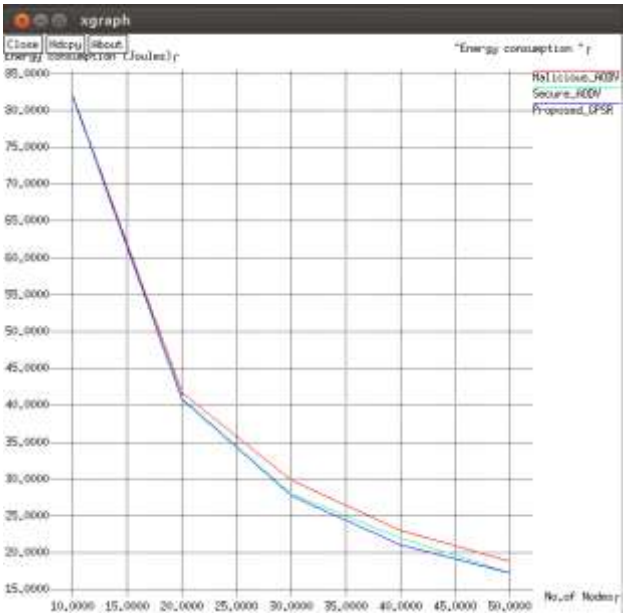

Figure 6: VANET Energy

Figure 7 represents the routing overhead where, x-axis represents the no. of nodes and y-axis represents the overhead. In this graph we define the overhead as the total bytes transmitted per successfully received packet. The total transmitted packets include beaconing messages, data packets and other packets that allow the proper functioning of the Protocols. The common network overhead of the three protocols is the use of the proactive beaconing to build the neighboring tables; this latter grows proportionally as the vehicle density traffic increase. We can observe that our approach generate the lowest overhead. In AODV the high overhead observed is due to its route discovery phase that the route request packets flood to the network for searching the route and the high node mobility leads to disrupted network and the overhead significantly increase due to repairs of broken routes. In GPSR the overhead is increased by the mechanism proposed by the authors to detect if a node is located at an intersection or not to play the role of a coordinate.

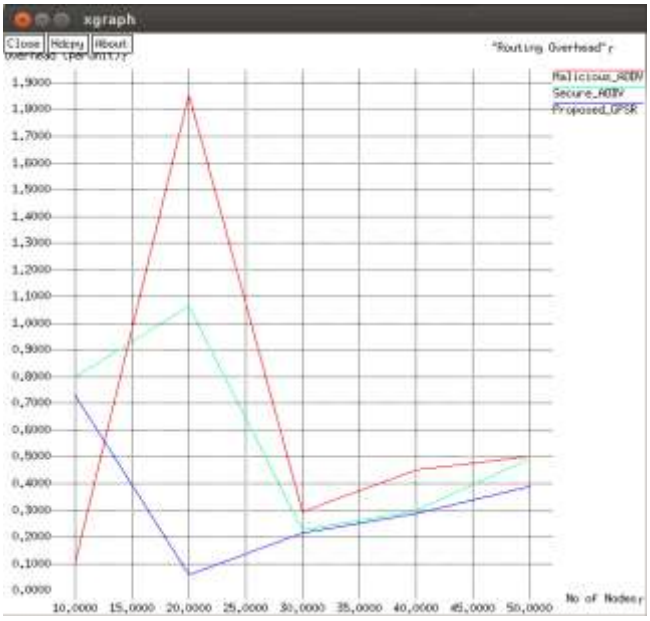

Figure 7: VANET Overhead

Figure 8 represents the packet delivery ratio, where, x-axis represents the no. of nodes and y-axis represents the PDR. The Packet Delivery Ratio (PDR) with different densities of vehicles. The Packet delivery ratio represents the ratio of packets delivered to the destinations to those generated by the sources. For all traffic densities, our proposed approach outperforms GPSR and AODV. This is because we have take into account the inclusion of the density traffic of the network to avoid network disconnection and we have also considered the presence of radio obstacles (which bloc signal transmissions) to avoid forwarding to a wrong segment which could result in the loss of the packet. We can see also that more packets are delivered as vehicles number increases

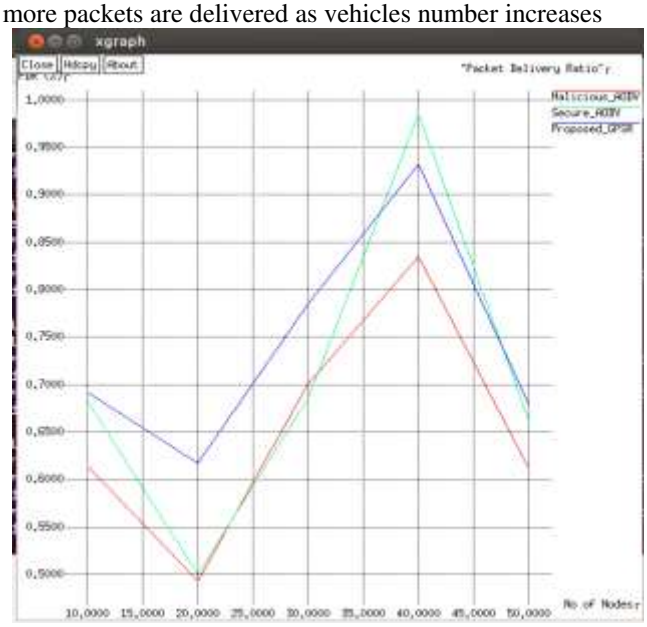

Figure 8: VANET PDR

Figure 9 represents the throughput where, x-axis represents the no. of nodes and y-axis represents the throughput. The aggregate throughput is calculated the Total no. of bytes successfully received at the sink divided by the total time duration. Calculating Aggregate throughput by using malicious_AODV and secure_AODV and proposed GPSR methods.

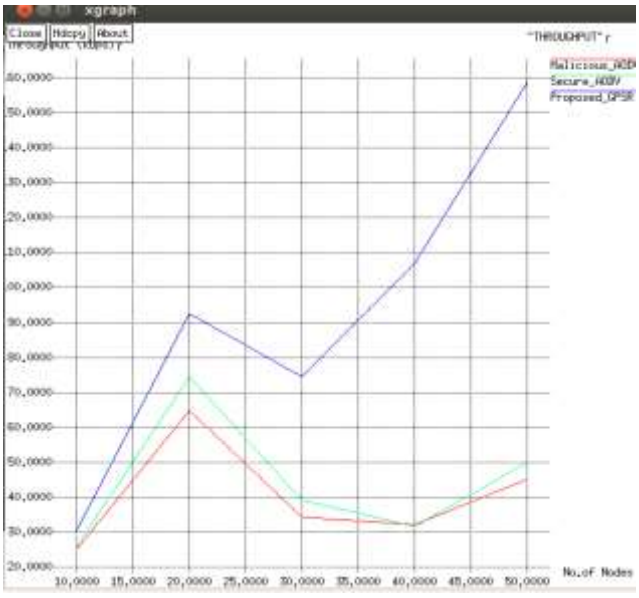

Figure 9: VANET Throughput

VII. Conclusion

This paper presented an overview and tutorial of various issues in VANET. Various types of research challenges are highlighted in context of vehicular communication. In particular, this paper presented a review of VANET architecture, transmission modelling, mathematical aspects of signal modelling, routing protocols and security. A comparative analysis of different routing algorithms in the field of VANET has been presented. It also highlighted the main issues in routing algorithms. This paper introducing use the concept of hash function to detect misbehaving node in VANET. This paper uses the concept of Greedy Perimeter Stateless Routing algorithm for routing in VANET. The performance metrics for routing algorithms, discussed in this paper, were PDR with respect to average velocity of vehicles, node density and system throughput. The other parameters of interest discussed widely in the paper were average end-to-end delay and routing overheads.

References

[1] Mohamed Watfa, Advances in Vehicular Ad-Hoc Networks: Developments and Challenges.: IGI Global, 2010.
[2] Ganesh S. Khekare and Apeksha V. Sakhare, "Intelligent Traffic System for VANET: A Survey," International Journal of Advanced Computer Research, vol. 2, Number-4, no. 6, pp. 99-102, December 2012.
[3] Rakesh Kumar and Mayank Dave, "A Review of Various VANET Data Dissemination Protocols," International Journal of u- and e- Service, Science and Technology, vol. 5, no. 3, pp. 27-44, 2012.
[4] Sherali Zeadally, Ray Hunt, Yuh Shyan Chen, Angela Irwin, and Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results and challenges," Springer Science, Business Media, LLC, p. 25, 2010.
[5] Prassant Mohapatra and Srikanth V. Krishnamurthy, Ad Hoc Networks : Technologies and Protocols. Boston, USA: Springer, 2005.
[6] Mohammad Jalil Piran, G. Rama Murthy, and G. Praveen Babu, "Vehicular Ad Hoc and Sensor Networks; Principles and Challenges," International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), vol. 2, no. 2, pp. 38-49, 2011.
[7] Francisco J. Martinez, Chai Keong Toh, Juan Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)," Wireless Communictions and Mobile Computing, vol. 11, pp. 813–828, 2011.
[8] Punam Bedi and Vinita Jindal, "Use of Big Data Technology in Vehicular Ad-hoc Networks," in International Conference on Advances in Computing, Communications and Informatics (ICACCI- 2014), Greater Noida, India, 2014, pp. 1677 – 1683.
[9] K. R. Jothi and A. Ebenezer Jeyakumar, "Optimization and Qualityof-Service Protocols in VANETs: A Review," Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, pp. 275-284, 2015.
[10] Hassnaa Moustafa and Yan Zhang, Vehicular networks: techniques, standards, and applications.: Auerbach publications, 2009.
[11] U.S. Department of Transporatation, "Intelligent Transportation System (ITS) Home," january 2014. [Online]. http://www.its.dot.gov/index.htm
[12] Peppino Fazio, Floriano de Rango, and Andrea Lupia, "Vehicular Networks and Road Safety: an Application for Emergency/Danger Situations Management Using the WAVE/802.11p Standard," Advances in Electrical and Electronic Engineering, pp. 357-364, 2013.
[13] James Bernsen, D. Mnivannan, "Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification", in journal of Pervasive and Mobile Computing 5 (2009)
[14] C K Toh, Ad Hoc Mobile Wireless Networks.: Prentice Hall Publishers, 2002.

Priyanka Tiwari , Department of Computer Science and Engineering, M.Tech Scholar, Kanpur Institute of Technology, Kanpur, India.
Mr. Rahul Gupta, Assistant Professor, Department of Computer Science and Engineering, Kanpur Institute of Technology, Kanpur, India